UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

715 BROOKS AVENUE, CINCINNATI, OHIO 45215

Case No. **1:23-mj-00002**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-1

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252(a)(2) & (a)(4)(B); 18 U.S.C. §§ 2252A(a)(2)(A) & (a)(5)(B)	Receipt, Distribution, Possession/Access with intent to view a visual depiction of a minor engaged in sexually explicit conduct

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

KIMBERLY A WALLACE Digitally signed by KIMBERLY A WALLACE Date: 2023.01.04 11:37:09 -05'00'

Applicant's signature

Kimberly Wallace, Special Agent HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime Video Conference *(specify reliable electronic means)*.

Date: **Jan 4, 2023**

Stephanie K. Bowman

Judge's signature

City and state: Cincinnati, Ohio

Stephanie K. Bowman, United States Magistrate Judge

Printed name and title

ATTACHMENT A-1

DESCRIPTION OF LOCATION TO BE SEARCHED

The property to be searched is located at 715 Brooks Avenue, Cincinnati, Ohio 45215 (the **SUBJECT PREMISES**), including all outbuildings and structures on this property, as well as all vehicles parked on this property and its driveway. The **SUBJECT PREMISES** is located on the west side of Brooks Avenue. The **SUBJECT PREMISES** is a light gray brick two-story home with black/dark colored shutters. The numbers "715" are affixed to the right of the front door and "715" is also affixed to a partial fence/wall to the left of the driveway of the **SUBJECT PREMISES**. An outbuilding/detached garage appears at the end of the driveway and is located to the northwest of the **SUBJECT PREMISES**.

ATTACHMENT B-1

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4)(B), 2252A(a)(2), and 2252A(a)(5)(B) (the "Target Offenses"), including:

a. All visual depictions of child pornography, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C. § 2256;

b. Child erotica;

c. Records and information relating to any computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

d. Records and information relating to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C § 2256, or pertaining to an interest in child pornography or sexual interest in minors, whether possessed, transmitted, or received;

e. Records and information relating to the ownership or possession of the **SUBJECT PREMISES**;

f. Records and information relating to Kik accounts "averagestud2", "jeffham123456", "jhamsuperdude", "jeffhamilton14", "jeffhamilton410", "newtothiscincy", "jefhami", "jehamil", "hamilton.je", and "jsmithsupyall", and any other accounts used in furtherance of the Target Offenses;

g. Records and information relating to the identity of "Jeff B", "Jeff Hamilton", "J H", "Je Ham", "J B", "Jeff Ham", and "Jeff Smith (pm)";

h. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF THE RESIDENCE LOCATED AT: 715 BROOKS AVENUE, CINCINNATI, OHIO 45215	Case No. **1:23-mj-00002** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kimberly Wallace, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 715 Brooks Avenue, Cincinnati, Ohio 45215 (the "**SUBJECT PREMISES**") and the person of **Jeffrey Scott BAILEY** ("**BAILEY**"), further described in Attachments A-1 and A-2, for the things described in Attachments B-1 and B-2.

2. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since June 2010, and am currently assigned to the HSI Resident Agent in Charge Cincinnati, Ohio office. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography

(as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on the facts in this Affidavit, I submit that there is probable cause to believe that contraband or evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the **SUBJECT PREMISES** and on the person of **BAILEY**.

PERTINENT FEDERAL CRIMINAL STATUTES

4. This investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual

depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child

pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. Pursuant to Title 18, United States Code, Section 2256, the term sexually explicit conduct includes the lascivious exhibition of the genitals or pubic area of any person.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachments B-1 and B-2:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction

involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software,

documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the

Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital

devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to another device using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows a computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various

types—to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person or in an individual's vehicle. Smartphones and/or mobile phones are often carried on an individual's person. Additionally, devices and other electronic storage media can be found in an individual's vehicle.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this

information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE, DISTRIBUTE, AND/OR POSSESS CHILD PORNOGRAPHY

7. As a result of my training and experience in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt, distribution, and possession of child pornography.

a. These individuals may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasizing while viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. These individuals may collect sexually explicit or suggestive materials, in a variety of media, including digital and electronic media, photographs, magazines, motion pictures, video tapes, books, sliders, drawings, and/or other visual media. These individuals often use these materials for their own sexual arousal and gratification.

Furthermore, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. To the extent these individuals possess and maintain "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., they almost always maintain those hard copies in the privacy and security of their home. They typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. Likewise, these individuals often maintain their digital or electronic collections of child sexual exploitation images in a safe, secure, and private environment, such as a computer and surrounding area, or on cellular telephones. These collections are often maintained for several years and are kept close by, usually at the individual's residence, on his or her person, or in his or her vehicles, to enable the individual to view the collection, which is valued highly. It is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices to obtain, store, or share their collections. Increasingly, individuals who view child pornography are utilizing laptop computers and other smaller devices, such as cellular telephones, iPads, and tablets to do their computing.

e. These individuals also may correspond with and/or meet others to share information and materials; are rarely able to completely destroy correspondence from other child pornography distributors/collectors; conceal correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. These individuals prefer not to be without their child sexual exploitation images for any prolonged time period. Collectors will take their collection with them if they change residences, as the collection is considered to be a prized possession. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. That said, there are individuals with a sexual interest in children who download and view digital images of child sexual exploitation, and delete them in order to avoid detection by law enforcement or other people. However, even in cases where these images are deleted, or concealed via encryption software, forensic examiners can sometimes use specialized tools to recover the deleted files or access encrypted files.

g. These individuals often use specialized software to conceal the existence of evidence and/or destroy said evidence. There are a variety of different programs that an individual can use to accomplish these objectives, many of which are free. Additionally, these individuals have been known to store child pornography in unconventional physical locations, as well as in unusual digital locations on computers and cellular phones. These

files and folders, or applications, have been misnamed or renamed in an attempt to mislead investigators.

h. These individuals will often download and store images of children they know or with whom they have communicated, as well as their communications with those children. The images may not necessarily be pornographic or obscene in nature; however, they are often used for the individuals' sexual gratification.

PROBABLE CAUSE

8. In 2019 and 2020 HSI Cincinnati received multiple leads from the HSI Cyber Crimes Center (C3) regarding Kik Interactive Inc. (hereinafter "Kik") accounts potentially involved with the possession and distribution of child pornography on the Kik mobile chat application. The Kik legal department provided the images, account information, and Internet Protocol (IP) address log history of the suspect users to the Royal Canadian Mounted Police (RCMP) who, based on IP address geolocation, referred the information to the HSI C3 for dissemination to corresponding HSI Field Offices in the United States for investigation. HSI C3 referred multiple Kik accounts to HSI Cincinnati based on IP address geolocation information.

9. Kik advertises itself as "the first smartphone messenger with a built-in browser." Kik Messenger allows its users to "talk to your friends and browse and share any web site with your friends on Kik." Kik believes it is at the forefront of the "new era of the mobile web." Kik was founded in 2009 by a group of University of Waterloo students who started a company designed to "shift the center of computing from the PC to the phone." According to the website, Kik Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers,

Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control of with whom they communicate. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even more with mobile web pages.

10. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads and is available on the Google PlayStore for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

11. In general, providers like Kik ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address. However, this information is not verified by Kik.

12. Kik typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. Kik often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. In addition, generally Kik maintains at least the last 30 days of all communications for each Kik user and will produce these records when requested pursuant to a search warrant.

13. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

14. In October 2019, Kik was purchased by MediaLab, a company operating in the United States. Given the ability for users to create multiple accounts that are not linked to a specific mobile device (i.e., a phone number), it has become a popular app used by people involved in the collection, receipt, and distribution of child pornography.

averagestud2

15. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "Jeff B", username "averagestud2", email address "jham1153@aol.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child pornography, as described herein.

16. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. The image distributed by "averagestud2" is described as follows:

a. An image of a young female, wearing only a bra with no pubic hair, bent over revealing her vagina and anus. The female was looking back at the camera with her arm in the air. A watermark on the bottom right of the image stated,

"NewIncest.com". Based on my training and experience, I believe that this image depicts child pornography.

17. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 184.54.243.250 was used by "averagestud2" on August 2, 2019, to send the above-described child pornography image.

18. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 184.54.243.250, used on August 2, 2019, to send a child pornography image, was registered to Charter Communications, Inc.

19. On or about February 13, 2020, an administrative summons was issued to Charter Communications, Inc in regard to IP address 184.54.243.250. A review of the results identified the subscriber as, Jeffrey **BAILEY** (513-886-2598), 715 Brooks Ave, Cincinnati, OH 45215, which is the address of the **SUBJECT PREMISES**.

jeffham123456

20. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "Jeff Hamilton", username "jeffham123456", email address "superdudeagain@gmail.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child pornography, as described herein.

21. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. The image distributed by "jeffham123456" is described as follows:

a. An image of a young female, wearing only a bra with no pubic hair, bent over revealing her vagina and anus. The female was looking back at the camera with her arm in the air. A label on the bottom right of the image stated, "NewIncest.com". The image appears to be the same image as described in Paragraph 16a. Based on my training and experience, I believe that this image depicts child pornography.

22. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 66.42.134.90 was used by "jeffham123456" on August 13, 2019, to send the above-described child pornography image.

23. A query of the ARIN online database revealed that IP address 66.42.134.90, used on August 13, 2019, to send the child pornography image, was registered to Fuse Internet (Cincinnati Bell Telephone).

24. On or about February 26, 2020, an administrative summons was issued to Cincinnati Bell Telephone in regard to IP address 66.42.134.90. A review of the results identified the subscriber as, Jeffrey **BAILEY** (513-886-2598), 6929 Tylersville Road, St 11, West Chester, OH 45069.

a. An open internet query for the above-referenced address listed multiple businesses including Real Estate Professionals, LLC from the Better Business Bureau and Realtor.com.

b. An open internet query for the above-referenced subscriber's telephone number listed Jeffrey **BAILEY**, as a real estate agent, from Zillow.com.

jhamsuperdude

25. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "Jeff Hamilton", username "jhamsuperdude", email address "jeffhamilton146@aol.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child pornography, as described herein.

26. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. The image distributed by "jhamsuperdude" is described as follows:

a. An image of a young female, wearing only a bra with no pubic hair, bent over revealing her vagina and anus. The female was looking back at the camera with her arm in the air. A label on the bottom right of the image stated, "NewIncest.com". The image appears to be the same image as described in Paragraph 16a. Based on my training and experience, I believe that this image depicts child pornography.

27. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 66.42.134.90 was used by "jhamsuperdude" on August 23, 2019, to send the above-described child pornography image.

28. A query of the ARIN online database revealed that IP address 66.42.134.90, used on August 23, 2019, to send the child pornography image, was registered to Fuse Internet (Cincinnati Bell Telephone).

29. On or about February 26, 2020, an administrative summons was issued to Cincinnati Bell Telephone in regard to IP address 66.42.134.90. A review of the results identified the subscriber as, Jeffrey **BAILEY** (513-886-2598), 6929 Tylersville Road, St 11, West Chester, OH 45069.

a. An open internet query for the above-referenced address listed multiple businesses including Real Estate Professionals, LLC from the Better Business Bureau and Realtor.com.

b. An open internet query for the above-referenced subscriber's telephone number listed Jeffrey **BAILEY**, as a real estate agent, from Zillow.com.

jeffhamilton14

30. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "J H", username "jeffhamilton14", email address "je.hamm@aol.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child pornography, as described herein. Subscriber information also included IP addresses utilized to access the Kik account which included 66.42.134.90 (as referenced in Paragraphs 22 and 27) and 184.54.255.137 on August 25, 2019.

31. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. The image distributed by "jeffhamilton14" is described as follows:

a. An image of a young female, wearing only a bra with no pubic hair, bent over revealing her vagina and anus. The female was looking back at the camera with her arm in the air. A label on the bottom right of the image stated, "NewIncest.com". The image appears to be the same image as described in Paragraph 16a. Based on my training and experience, I believe that this image depicts child pornography.

32. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 208.54.90.135 was used by "jeffhamilton14" on August 26, 2019, to send the above-described child pornography image.

33. A query of the ARIN online database revealed that IP address 208.54.90.135, used on August 26, 2019, to send the child pornography image, was registered to T-Mobile USA, Inc.

34. On or about February 26, 2020, an administrative summons was issued to T-Mobile in regard to IP address 208.54.90.135. A review of the results revealed that T-Mobile was unable to determine subscriber information.

35. A query of the ARIN online database revealed that IP address 184.54.255.137 (which was utilized to access the account as referenced in Paragraph 30) was registered to Charter Communications, Inc.

36. On or about February 13, 2020, an administrative summons was issued to Charter Communications in regard to IP address 184.54.255.137. A review of the results identified the subscriber as, Jeffrey **BAILEY** (513-886-2598), 715 Brooks Ave, Cincinnati, OH 45215, which is the address of the **SUBJECT PREMISES**.

jeffhamilton410

37. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "Jeff Hamilton", username "jeffhamilton410", email address "jeffhamilton410@aol.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child erotica, as described herein.

38. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. The image distributed by "jeffhamilton410" is described as follows:

a. An image of a nude pre-pubescent aged female, laying nude on her side, facing the camera. Based on my training and experience, I believe that this image depicts child erotica.

39. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 184.54.255.137 was used by "jeffhamilton410" on August 30, 2019, to send the above-described child erotica image.

40. A query of the ARIN online database revealed that IP address 184.54.255.137, used on August 30, 2019, to send the child erotica image, was registered to Charter Communications, Inc.

41. On or about March 3, 2020, an administrative summons was issued to Charter Communications, Inc in regard to IP address 184.54.255.137. A review of the results identified

the subscriber as, Jeffrey **BAILEY** (513-886-2598), 715 Brooks Ave, Cincinnati, OH 45215, which is the address of the **SUBJECT PREMISES**.

newtothiscincy

42. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "Je Ham", username "newtothiscincy", email address "je.hamilton@aol.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child pornography, as described herein. Subscriber information also included IP addresses utilized to access the Kik account which included 66.42.134.90 (as referenced in Paragraphs 22 and 27).

43. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. The image distributed by "newtothiscincy" is described as follows:

a. An image of a nude pre-pubescent aged female, straddling a pillow, and facing the camera. The female, and room/bedding material, appears to be the same female, but in a different pose, as the image described in Paragraph 38a. Based on my training and experience, I believe that this image depicts child pornography.

44. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 184.54.255.137 was used by "newtothiscincy" on September 18, 2019, to send the above-described child pornography image.

45. A query of the ARIN online database revealed that IP address 184.54.255.137, used on September 18, 2019, to send the child pornography image, was registered to Charter Communications, Inc.

46. On or about March 3, 2020, an administrative summons was issued to Charter Communications, Inc in regard to IP address 184.54.255.137. A review of the results identified the subscriber as, Jeffrey **BAILEY** (513-886-2598), 715 Brooks Ave, Cincinnati, OH 45215, which is the address of the **SUBJECT PREMISES**.

jefhami

47. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "J H", username "jefhami", email address "jeffhamilton705@aol.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child erotica, as described herein. Subscriber information also included IP addresses utilized to access the Kik account which included 66.42.134.90 (as referenced in Paragraphs 22 and 27).

48. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. The image distributed by "jefhami" is described as follows:

a. A pubescent minor female, nude, standing upright and facing the camera. The female had no breast development and minimal pubic hair. Based upon my training and experience, I believe that this image depicts child erotica.

49. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 184.54.255.137 was used by "jefhami" on September 26, 2019, to send the above-described child erotica image.

50. A query of the ARIN online database revealed that IP address 184.54.255.137, used on September 26, 2019, to send the child erotica image, was registered to Charter Communications, Inc.

51. On or about March 3, 2020, an administrative summons was issued to Charter Communications, Inc in regard to IP address 184.54.255.137. A review of the results identified the subscriber as, Jeffrey **BAILEY** (513-886-2598), 715 Brooks Ave, Cincinnati, OH 45215, which is the address of the **SUBJECT PREMISES**.

jehamil

52. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "J B", username "jehamil", email address "jeffhamilton796@aol.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child erotica, as described herein.

53. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. The image distributed by "jehamil" is described as follows:

a. A pubescent minor female, nude, standing upright and facing the camera. The female had no breast development and minimal pubic hair. The image appears to

be the same image as described in Paragraph 48a. Based upon my training and experience, I believe that this image depicts child erotica.

54. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 184.54.255.137 was used by "jehamil" on October 1, 2019, to send the above-described image.

55. A query of the ARIN online database revealed that IP address 184.54.255.137, used on October 1, 2019, to send the image, was registered to Charter Communications, Inc.

56. On or about March 3, 2020, an administrative summons was issued to Charter Communications, Inc in regard to IP address 184.54.255.137. A review of the results identified the subscriber as, Jeffrey **BAILEY** (513-886-2598), 715 Brooks Ave, Cincinnati, OH 45215, which is the address of the **SUBJECT PREMISES**.

hamilton.je

57. Your Affiant has reviewed subscriber information, provided by Kik, which showed that a Kik user with the registered name "Jeff Ham", username "hamilton.je", email address "hamilton.je@aol.com", and utilized phone brand and model Android SM-J700T, used Kik to send an image of child pornography, as described herein. Subscriber information also included IP addresses utilized to access the Kik account which included 184.54.255.137 (as referenced in Paragraphs 39, 44, 49, and 54).

58. Along with subscriber information, Kik provided a copy of the uploaded image to the RCMP. Your Affiant reviewed the same image that Kik had provided to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik

personnel before it was reported to the RCMP. The image distributed by "hamilton.je" is described as follows:

a. An image of a pre-pubescent aged female, with slight breast development and no pubic hair, naked lying down with her legs open revealing her genitals. Based on my training and experience, I believe that this image depicts child pornography.

59. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 66.42.134.90 was used by "hamilton.je" on October 10, 2019, to send the above-described child pornography image.

60. A query of the ARIN online database revealed that IP address 66.42.134.90, used on October 10, 2019, to send the child pornography image, was registered to Fuse Internet (Cincinnati Bell Telephone).

61. On or about February 26, 2020, an administrative summons was issued to Cincinnati Bell Telephone in regard to IP address 66.42.134.90 A review of the results identified the subscriber as, Jeffrey **BAILEY** (513-886-2598), 6929 Tylersville Road, St 11, West Chester, OH 45069.

62. Your Affiant has learned that Kik was alerted to the child pornography images, referenced in the above nine (9) Kik accounts, through use of Microsoft's PhotoDNA technology. According to the Kik Glossary, Kik used PhotoDNA to automatically scan user-uploaded files in order to flag images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When PhotoDNA detected a suspected child pornography file, it created a Report and sent it to the Kik Law Enforcement team. According to information provided by a Kik Law Enforcement Response Team Lead, all

suspected child pornography images and videos reported via a PhotoDNA Report, as well as any related user communications, were visually reviewed by a member of the Kik Law Enforcement Response team before a report was forwarded to law enforcement authorities. Kik trained employees comprising its Law Enforcement Response team on the legal obligation to report apparent child pornography. The Team was trained on the Canadian statutory definition of child pornography and how to recognize it on Kik products and services. Kik voluntarily made reports to law enforcement in accordance with that training. After Kik discovered the suspected child pornography, Kik removed the content from its communications system and closed the user's accounts.

Background on NCMEC

63. The National Center for Missing & Exploited Children (NCMEC) is a non-governmental organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography. Companies that suspect that child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip. To make such a report, a company providing services on the internet, electronic service providers (ESPs) and internet service providers (ISPs), can go to an online portal known as the CyberTipline that NCMEC has set up for the submission of these tips. The ISP or ESP then can provide to NCMEC information concerning the child exploitation activity it believes to have occurred, including the incident type, the incident time, any screen or user names associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. The ISP or ESP may also upload to NCMEC any files it collected in connection with the activity. Using

publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ISP or ESP provides, such as IP addresses. NCMEC then packages the information from the ISP and ESP along with any additional information it has, such as previous related cybertips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

CyberTipline Report 135711300

64. In November 2022, HSI Cincinnati received NCMEC CyberTip Report 135711300 with an incident type of child pornography. NCMEC received the report on or about September 29, 2022, from MediaLab/Kik, an ESP. The reported account included registered name "Jeff Smith (pm)", username "jsmithsupyall", email address "niceguy301751@yahoo.com", and utilized phone brand and model Android SM-A115U. The ESP reported that the account (jsmithsupyall) sent nine (9) files to another user via private chat message. The ESP reported that the ESP viewed all nine (9) files. Several of the files are described as follows:

a. File named, c2502070-17cb-4078-a95e-c13c412d2cfc.jpg was an image of a pre-pubescent aged female, with slight breast development and no pubic hair, nude and sitting down with her legs open revealing her genitals. Based on my training and experience, I believe that this image depicts child pornography. This image was distributed on or about September 16, 2022, from IP address 184.54.255.137.

b. Files named, 06d09fda-b083-4198-9d63-26b6bdeeb898.jpg and eba97397-c474-4236-b925-4c63fb16e17d.jpg, both files appeared to be the same image (and reflected the same hash value) and depicted a minor female with slight breast

development, nude from the abdomen up, facing the camera. Based on my training and experience, I believe that this image depicts child erotica. This image was distributed on or about September 15 and 16, 2022, from IP address 184.54.255.137.

c. File named, e09c636f-6b3d-4f9e-a8ba-16f7eef040c3.jpg, depicted a minor female with slight breast development, nude from the abdomen up, facing the camera. Based on my training and experience, I believe that this image depicts child erotica. This image was distributed on or about September 16, 2022, from IP address 184.54.255.137.

d. Files named, b559e971-c470-411a-a0b2-4f758699830c.jpg and a935f6d9-9e33-468c-a7a9-c350aa1bded6.jpg, both files appeared to be the same image (and reflected the same hash value) and depicted a minor female wearing only a shirt, on her knees and one hand on the ground, facing the camera while taking a photo. Based on my training and experience, I believe that this image depicts child erotica. This image was distributed on or about September 12 and 16, 2022, from IP address 184.54.255.137.

65. All nine (9) files were uploaded from IP address 184.54.255.137 on four different dates in September 2022. A query of the ARIN online database revealed that IP address 184.54.255.137, used on multiple dates in September 2022 was registered to Charter Communications, Inc.

66. On or about November 9, 2022, an administrative summons was issued to Charter Communications, Inc in regard to IP address 184.54.255.137. A review of the results identified

the subscriber as, Jeffrey **BAILEY** (513-886-2598), 715 Brooks Ave, Cincinnati, OH 45215, which is the address of the **SUBJECT PREMISES**.

Research

67. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for the **SUBJECT PREMISES** (715 Brooks Ave, Cincinnati, Ohio). These public records indicated that the **SUBJECT PREMISES** is the current residence for **BAILEY**.

68. On or about November 9, 2022, a query with Ohio's Bureau of Motor Vehicles revealed that an individual named Jeffrey Scott **BAILEY** with a date of birth of XX/XX/1973 lists a residential address of the **SUBJECT PREMISES**.

69. An open internet query for "Jeff Bailey" resulted in a Twitter account (@CoachJeffBailey) from Wyoming, OH, which depicted multiple images of BAILEY (as compared to his driver's license image). A post on "Oct 5" stated in part, "I have started a new chapter in my coaching career as the Head Coach of the Middletown Christian Eagles." The accompanying image to the post included an image of BAILEY along with the title of Basketball Head Coach.

70. As of November 14, 2022, the Hamilton County Auditor's website listed Jeffrey and Jennifer BAILEY as the current owners of the **SUBJECT PREMISES**.

71. On or about November 29, 2022, law enforcement surveillance observed **BAILEY** walking a dog and rolling a trashcan from the curb and up the driveway towards the **SUBJECT PREMISES**

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

72. As described above and in Attachments B-1 and B-2, this application seeks permission to search for certain records that might be found on the **SUBJECT PREMISES** and on the person of **Jeffery BAILEY**, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

73. Given the information set forth above, I submit that if a computer or electronic storage medium is found on the **SUBJECT PREMISES** or the person of **BAILEY**, there is probable cause to believe those records referenced above may still be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

74. As further described in Attachments B-1 and B-2, this application seeks permission to locate not only computer files and electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on any computer or electronic storage medium in the **SUBJECT PREMISES** or on the person of **BAILEY** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks

and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online usernames, nicknames, and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with

user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

75. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as

a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

76. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which

create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

77. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying computers and electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

78. Because it appears that several people share the **SUBJECT PREMISES** as a residence, it is possible that the **SUBJECT PREMISES** will contain computers or electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant

could be found on any of those computers or electronic storage media, the warrant applied for would permit the seizure and review of those items as well.

SEARCH METHODOLOGY TO BE EMPLOYED

79. All computers, other computer hardware, computer software, and any form of electronic storage media that could contain evidence described in this warrant may be seized for an off-site search for evidence that is described in the attachments of this warrant. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.

80. The search procedure of electronic data contained in computers, other computer hardware, computer software, and/or electronic storage media may include the following techniques (the following is a non-exhaustive list, as other search procedures may be used):

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. On-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. Examination of all of the data contained in such computers, other computer hardware, computer software, or electronic storage media to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. Surveying various file directories and the individual files they contain;

f. Opening files in order to determine their contents;

g. Scanning storage areas;

h. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachments B-1 and B-2; and

i. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachments B-1 and B-2.

81. Contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

82. Because it is expected that the computers, other computer hardware, computer software, and any form of electronic storage media may constitute (1) instrumentalities of the

offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case.

a. Because of the large storage capacity as well as the possibility of hidden data within the computers, other computer hardware, and any form of electronic storage media, it is anticipated that there will be no way to ensure that contraband-free evidence could be returned to the user/possessor of the computer, other computer hardware, or any form of electronic storage media, without first wiping such evidence clean. Wiping the original evidence clean would mean that the original evidence would be destroyed and thus, would be detrimental to the investigation and prosecution of this case.

b. Further, because investigators cannot anticipate all potential defenses to the offenses in this Affidavit, and as such, cannot anticipate the significance of the evidence that has been lawfully seized pursuant to this warrant, it is requested that all seized evidence be retained by law enforcement until the conclusion of legal proceedings or until other order of the court.

c. If after careful inspection investigators determine that such computers, other computer hardware, computer software, and electronic storage media do not contain or constitute (1) instrumentalities of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

CONCLUSION

83. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), as described in Attachments B-1 and B-2, are located at the locations described in Attachments A-1 and A-2. I respectfully request that this Court issue a search warrant for the locations described in Attachments A-1 and A-2, authorizing the seizure and search of the items described in Attachments B-1 and B-2.

84. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the **SUBJECT PREMISES** and the person of **BAILEY**. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

KIMBERLY A WALLACE

Digitally signed by KIMBERLY A WALLACE
Date: 2023.01.04 11:37:54 -05'00'

Kimberly Wallace
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 4th day of January 2023.
via electronic means, specifically Facetime video.

Stephanie K. Bowman

HON. STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE COURT JUDGE

ATTACHMENT A-1

DESCRIPTION OF LOCATION TO BE SEARCHED

The property to be searched is located at 715 Brooks Avenue, Cincinnati, Ohio 45215 (the **SUBJECT PREMISES**), including all outbuildings and structures on this property, as well as all vehicles parked on this property and its driveway. The **SUBJECT PREMISES** is located on the west side of Brooks Avenue. The **SUBJECT PREMISES** is a light gray brick two-story home with black/dark colored shutters. The numbers "715" are affixed to the right of the front door and "715" is also affixed to a partial fence/wall to the left of the driveway of the **SUBJECT PREMISES**. An outbuilding/detached garage appears at the end of the driveway and is located to the northwest of the **SUBJECT PREMISES**.

ATTACHMENT B-1

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4)(B), 2252A(a)(2), and 2252A(a)(5)(B) (the "Target Offenses"), including:

a. All visual depictions of child pornography, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C. § 2256;

b. Child erotica;

c. Records and information relating to any computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

d. Records and information relating to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C § 2256, or pertaining to an interest in child pornography or sexual interest in minors, whether possessed, transmitted, or received;

e. Records and information relating to the ownership or possession of the **SUBJECT PREMISES**;

f. Records and information relating to Kik accounts "averagestud2", "jeffham123456", "jhamsuperdude", "jeffhamilton14", "jeffhamilton410", "newtothiscincy", "jefhami", "jehamil", "hamilton.je", and "jsmithsupyall", and any other accounts used in furtherance of the Target Offenses;

g. Records and information relating to the identity of "Jeff B", "Jeff Hamilton", "J H", "Je Ham", "J B", "Jeff Ham", and "Jeff Smith (pm)";

h. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.